WHAT IS CLAIMED IS:

1. A system for secure licensing of content to a user on a user network-enabled device, the system comprising:

at least one server network device communicatively coupled to the user network-enabled device;

wherein the at least one server network device is programmed to transfer selected content to the user network-enabled device; and

a license generator, the license generator being programmed to generate a license associated with the selected content, the license comprising access information for controlling the user network-enabled device to produce a user-perceptible form of the selected content when conditions defined by the access information are met and to inhibit production of a user-perceptible form of the selected content when conditions defined by the access information are not met.

2. The system recited in claim 1, wherein the at least one server network device is further programmed to receive at a first node on the network a request for content from the user network-enabled device at a second node on the network;

wherein the transfer of selected content comprises transferring the requested content in response to the receipt of the request at the second node.

3. The system recited in claim 1, wherein the content is encrypted.

4. The system recited in claim 1, wherein the at least one server network device is further programmed to receive at the first node on the network a request for the license from the user network-enabled device at the second node on the network; and

wherein the at least one server network device is further programmed to transfer the requested license to the user network-enabled device at the second node.

5. The system recited in claim 1, wherein the license is a data object.

6. The system recited in claim 5, wherein the data object comprises a plurality of data fields, at least a portion of the plurality of data fields containing the access information.

7. The system recited in claim 1, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

8. The system recited in claim 7, wherein the content rental model defines at least one of a specified period of time and a specified number of plays.

9. The system recited in claim 7, wherein the content rental model defines an unlimited number of plays on any user network-enabled device.

10. The system recited in claim 7, wherein the content rental model includes a watermark, the watermark allowing the user to rewind only a determined time interval from the current position in the movie.

11. The system recited in claim 1, further comprising at least one application server, the at least one application server being communicatively coupled to both the at least one server network device and the license generator;

wherein the at least one application server is programmed to receive the license request from the at least one server network and to transfer the license request to the license generator.

12. The system recited in claim 11, wherein the at least one application server is further programmed to provide business rules to the license generator, the business rules being included in the license request by the at least one application server before transferring the license request to the license generator, the business rules defining the types of licenses that the license generator may generate.

13. The system recited in claim 11, wherein the at least one application server is further programmed to gather and store personalization information about users.

14. The system recited in claim 11, wherein the at least one application server is further programmed to create dynamic Web pages.

15. The system recited in claim 11, further comprising a firewall situated between the at least one server network device and the at least one application server, the firewall preventing unauthorized access to the at least one application server.

16. The system recited in claim 11, further comprising a firewall situated between the at least one application server and the license generator, the firewall preventing unauthorized access to the license generator.

17. A method for secure licensing of content to a user on a user network-enabled device, the method comprising:

transferring selected content to the user network-enabled device; and

generating a license associated with the selected content, the license comprising access information for controlling the user network-enabled device to produce a user-perceptible form of the selected content when conditions defined by the access information are met and to inhibit production of a user-perceptible form of the selected content when conditions defined by the access information are not met.

18. The method recited in claim 17, wherein the license is a data object.

19. The method recited in claim 18, wherein the data object comprises a plurality of data fields, at least a portion of the plurality of data fields containing the access information.

20. The method recited in claim 17, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

21. A system for secure licensing of content to a user on a user network-enabled device, the system comprising:

at least one server network device communicatively coupled to the user network-enabled device;

wherein the at least one server network device is programmed to transfer a license associated with the content to the user network-enabled device, the license comprising access information which defines access rights to the content; and

wherein the user network-enabled device is programmed to provide media player and security technology, the media player and security technology verifying the access rights and allowing the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed and inhibiting the user network-enabled device from producing a user-perceptible form of the content when the content is not properly licensed.

22. The system recited in claim 21, wherein the media player and security technology comprises a media player for displaying the content in a user-perceptible form.

23. The system recited in claim 22, wherein the media player and security technology further comprises at least one of decryption code for decrypting encrypted content, a CODEC for decompressing compressed content, a monitor for displaying the media player to the user, and a hardware interface between the media player and the monitor.

24. The system recited in claim 23, wherein the media player and security technology further comprises digital rights management code for providing a secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor.

25. The system recited in claim 24, wherein the digital rights management code is protected against tampering by at least one of code obfuscation and anti-debugging techniques.

26. The system recited in claim 24, wherein the digital rights management code provides the secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor by performing an integrity check on at least one of the media player, the decryption code, the CODEC, the hardware interface, and the monitor in order to detect tampering.

27. The system recited in claim 26, wherein the digital rights management code inhibits the display of content in a user-perceptible form when at least one of the media player, the decryption code, the CODEC, the hardware interface, and the monitor do not pass the integrity check.

28. The system recited in claim 24, wherein the media player and security technology further comprises a protected database in communication with the digital rights management code;

wherein the protected database securely stores transferred licenses.

29. The system recited in claim 28, wherein the protected database is protected by encryption methods.

30. The system recited in claim 29, wherein the digital rights management code comprises a root key, the root key unlocking licenses within the protected database.

31. The system recited in claim 29, wherein the digital rights management code examines the access information within the unlocked license and determines the access rights to the content provided by the unlocked license.

32. The system recited in claim 22, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

33. The system recited in claim 32, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by enforcing compliance by the user with the content rental model contained in the unlocked license.

34. The system recited in claim 32, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing user network-

enabled device identification information in the unlocked license with the user network-enabled device on which the digital rights management code resides.

35. The system recited in claim 32, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing media player identification information in the unlocked license with the media player on the user network-enabled device on which the digital rights management code resides.

36. The system recited in claim 32, wherein the digital rights management code passes the encryption key contained in the unlocked license to the decryption code in order to decrypt the encrypted content.

37. A method for secure licensing of content to a user on a user network-enabled device, the method comprising:

transferring a license associated with the content to the user network-enabled device, the license comprising access information which defines access rights to the content; and

providing media player and security technology on the user network-enabled device, the media player and security technology verifying the access rights and allowing the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed and inhibiting the user network-enabled device from producing a user-perceptible form of the content when the content is not properly licensed.

38. The method recited in claim 37, wherein the media player and security technology comprises a media player for displaying the content in a user-perceptible form.

39. The method recited in claim 38, wherein the media player and security technology further comprises at least one of decryption code for decrypting encrypted content, a CODEC for decompressing compressed content, a monitor for displaying the media player to the user, and a hardware interface between the media player and the monitor.

40. The method recited in claim 39, wherein the media player and security technology further comprises digital rights management code for providing a secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor.

41. The method recited in claim 40, wherein the media player and security technology further comprises a protected database in communication with the digital rights management code;

wherein the protected database securely stores transferred licenses.

42. The method recited in claim 41, wherein the protected database is protected by encryption methods.

43. The method recited in claim 41, wherein the digital rights management code comprises a root key, the root key unlocking licenses within the protected database.

44. The method recited in claim 43, wherein the digital rights management code examines the access information within the unlocked license and determines the access rights to the content provided by the unlocked license.

45. The method recited in claim 38, wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content.

46. The method recited in claim 45, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by enforcing compliance by the user with the content rental model contained in the unlocked license.

47. The method recited in claim 45, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing user network-

enabled device identification information in the unlocked license with the user network-enabled device on which the digital rights management code resides.

48. The method recited in claim 45, wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing media player identification information in the unlocked license with the media player on the user network-enabled device on which the digital rights management code resides.

49. The method recited in claim 45, wherein the digital rights management code passes the encryption key contained in the unlocked license to the decryption code in order to decrypt the encrypted content.

50. A system for revoking a license to access content in a user-perceptible form on a user network-enabled device, the system comprising:

at least one revocation server, the at least one revocation server transferring to the user network-enabled device a revocation certificate;

wherein the revocation certificate comprises revocation information for controlling the user network-enabled device to inhibit production of a user-perceptible form of the content when conditions contained in the revocation information are satisfied.

51. The system recited in claim 50, further comprising media player and security technology for verifying the license and allowing the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed and inhibiting the user network-enabled device from producing a user-perceptible form of the content when the content is not properly licensed.

52. The system recited in claim 51, wherein the media player and security technology comprises a media player for displaying the content in a user-perceptible form.

53. The system recited in claim 52, wherein the media player and security technology further comprises at least one of decryption code for decrypting encrypted content, a CODEC for decompressing compressed content, a monitor for

displaying the media player to the user, and a hardware interface between the media player and the monitor.

54. The system recited in claim 53, wherein the media player and security technology further comprises digital rights management code for providing a secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor.

55. The system recited in claim 50, wherein the revocation certificate is a data object.

56. The system recited in claim 55, wherein the data object comprises a plurality of data fields, at least a portion of the plurality of data fields containing the revocation information.

57. The system recited in claim 56, wherein the revocation information comprises information about specific media player and security technology for which access to a user-perceptible form of the content is inhibited.

58. The system recited in claim 56, wherein the revocation information comprises information about specific content for which access in a user-perceptible form is inhibited.

59. The system recited in claim 51, wherein the media player and security technology further comprises a protected database in communication with the digital rights management code;

wherein the protected database securely stores transferred revocation certificates.

60. The system recited in claim 59, wherein the protected database is protected by encryption methods.

61. A method for communicating revocation certificates for revoking licenses to access content in a user-perceptible form on a user network-enabled device, the method comprising:

polling of a revocation server by the user network-enabled device, the revocation server containing a list of the revocation certificates; and

transferring the revocation certificates to the user network-enabled device.

62. The method recited in claim 61, wherein polling of the revocation server comprises polling the revocation server on a defined periodic basis.

63. The method recited in claim 62, wherein the defined periodic basis is once every ten days.

64. The method recited in claim 61, wherein transferring the revocation certificates to the user network-enabled device comprises transferring the revocation certificates to a protected database on the user network-enabled device.

65. The method recited in claim 64, wherein the protected database is protected by encryption methods.

66. The method recited in claim 62, further comprising inhibiting access to content in a user-perceptible form on the user network-enabled device when the revocation server has not been polled by the user network-enabled device within the defined period.

67. A method for communicating revocation certificates for revoking licenses to access content in a user-perceptible form on a user network-enabled device, the method comprising:

attaching a list of the revocation certificates to a requested license for content; and

transferring the requested license, over a network, to the user network-enabled device.

68. The method recited in claim 67, wherein attaching a list of the revocation certificates to a requested license for content comprises an application server attaching the list to the requested license.

69. The method recited in claim 67, wherein transferring the requested license to the user network-enabled device comprises transferring the requested license to a protected database on the user network-enabled device.

70. The method recited in claim 69, wherein the protected database is protected by encryption methods.

71. A method for authenticating a license to access content in a user-perceptible form on a user network-enabled device, comprising:

connecting to a server network device, the server network device being communicatively coupled to the user network-enabled device via a communication link;

comparing the content with content identification information contained in the license;

comparing the user network-enabled device with user network-enabled device identification information contained in the license; and

comparing the media player on the user network-enabled device with media player identification information contained in the license;

wherein the server network device is programmed to deny enablement of the license if the results of any of the comparisons are false and wherein the license resides on the user network-enabled device.

72. The method recited in claim 71, wherein connecting to the server network device comprises automatically connecting to the server network device when an attempt is made to access the content on the user network-enabled device.

73. The method recited in claim 71, wherein the comparisons are performed by media and security technology residing on the user network-enabled device.

74. A system for authenticating a license to access content in a user-perceptible form on a user network-enabled device, comprising:

a server network device communicatively coupled to the user network-enabled device via a communication link;

wherein the user network-enabled device is programmed for

connecting to the server network device via the communication link,

comparing the content with content identification information contained in the license,

comparing the user network-enabled device with user network-enabled device identification information contained in the license, and

comparing the media player on the user network-enabled device with media player identification information contained in the license, and

wherein the server network device is programmed to deny enablement of the license if the results of any of the comparisons are false and wherein the license resides on the user network-enabled device.

75. A method of restricting forwarding and reversing from a current position in a media file by a media player, comprising:

providing watermark information to a digital rights management system associated with the media player, the watermark information defining time intervals that limit forward and reverse progression through the media file from the current position in the media file; and

preventing forwarding and reversing of the media file beyond the limits defined by the time intervals.

76. The method recited in claim 75, wherein providing watermark information to the digital rights management system associated with the media player comprises providing the watermark information in a license data object within a protected data base, the license data object comprising access information associated with the movie file.

77. The method recited in claim 76, wherein the access information comprises a rental model.

78. The method recited in claim 77, wherein the rental model comprises the watermark information.

79. The method recited in claim 75, wherein the digital rights management system associated with the media player enforces the defined time interval limits by preventing progression of the movie file beyond the defined time interval limits.

80. The method recited in claim 79, wherein the digital rights management system associated with the media player enforces the defined time interval limits by tracking the user's progress in viewing the movie and restricting the reversing or fast-forwarding of the movie file by at least one of a hardware timer and a software timer.

81. The method recited in claim 75, wherein providing watermark information to the digital rights management system associated with the media player comprises providing watermarks at timed intervals in the movie file.

82. A business method for authenticating a license to access content in a user-perceptible form on a user network-enabled device, comprising:

providing a server network device, the server network device communicating with the user network-enabled device via a communication link;

offering, for a pre-defined remuneration, licenses associated with selected content and allowing, when the license is enabled, the user network-enabled device to access the selected content in a user-perceptible form in conformance with a selected rental model;

transferring the license associated with the selected content to the user network-enabled device, the license containing access information; and

comparing the access information contained in the transferred license to pre-defined information residing on the user network-enabled device;

wherein the server network device is programmed to deny enablement of the license if the result of the comparison is false.

83. A method for authorization of a license for content, the license being transferred from a first user network-enabled device to a second user network-enabled device, comprising:

transferring the content from the first user network-enabled device to the second user network-enabled device;

connecting the second user network-enabled device to a server network device, the server network device providing a user interface;

obtaining a license for the content, the license comprising access information; and

comparing the access information contained in the license to pre-defined information residing on the second user network-enabled device;

wherein the server network device is programmed to deny enablement of the license if the result of the comparison is false.

84. The method recited in claim 83, wherein connecting the second user network-enabled device to the server network device comprises connecting to a website on the Internet.

85. The method recited in claim 83, wherein transferring the content from the first user network-enabled device to the second user network-enabled device comprises copying the content to a computer readable disc, transporting the computer readable disc to the location of the second user network-enabled device, and copying the content from the computer readable disc to the second user network-enabled device.

86. The method recited in claim 83, wherein transferring the content from the first user network-enabled device to the second user network-enabled device comprises downloading the content from the first user network-enabled device to the second user network-enabled device over a network.

87. The method recited in claim 83, wherein transferring the content from the first user network-enabled device to the second user network-enabled device comprises the second user network-enabled device accessing content residing on the first user network-enabled device through a file-swapping user interface provided by the server network device, the file-swapping user interface allowing access to and transfer of content, the content residing on a plurality of user network-enabled devices, the plurality of user network-enabled devices being connected to the file-swapping user interface.

88. The method recited in claim 87, further comprising selection by the user of the second user network-enabled device of content residing on the first user network-enabled device and requesting transfer of the selected content to the second user network-enabled device.

89. The method recited in claim 88, further comprising transferring the selected content from the first user network-enabled device to the second network-enabled device.